IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	
v.	11-CR-397-S
JAMES RAYMONDA,	
Defendant.	

GOVERNMENT'S OBJECTIONS TO
THE MAGISTRATE JUDGE'S REPORT AND RECOMMENDATION

The United States of America, by and through WILLIAM J. HOCHUL, JR., United States Attorney for the Western District of New York, and the undersigned Assistant United States Attorney, hereby respectfully objects to the Report and Recommendation issued by Magistrate Judge Hugh B. Scott on April 5, 2013, recommending suppression of evidence obtained pursuant to a search warrant issued by the Honorable H. Kenneth Schroeder, Jr. The government also respectfully requests that the Court decline to adopt the portion of the Magistrate Judge's Report and Recommendation that recommends suppression of the defendant's statements to law enforcement agents as being "fruit of the poisonous tree" as the statements were voluntarily made by the defendant. The government further requests that the excited utterances made by the defendant in the presence of law enforcement officers, which were not the result of any questioning of the defendant by the officers, should not be suppressed.

PRELIMINARY STATEMENT

On December 21, 2011, a Grand Jury impaneled in the Western District of New York returned a five-count indictment with forfeiture allegation against the defendant charging violations of Title 18, United States Code, Sections 2252A(a)(2)(A) and 2252A(a)(5)(B) for receipt and possession of child pornography, that is, images of minor children engaged in sexually explicit conduct as defined in Title 18, United States Code, Section 2256. Based upon the defendant's motion to suppress evidence obtained pursuant to a search warrant issued in this matter and his statements to law enforcement agents, a suppression hearing was held by the Court over the course of several days with witness testimony being heard on August 7, 2012, October 18, 2012, and November 14, 2012.

The defendant has moved to suppress evidence related to the defendant's possession of child pornography obtained pursuant to the search warrant issued by Magistrate Judge H. Kenneth Schroeder, Jr., on October 27, 2011. In doing so, the defendant claims that the search warrant that Magistrate Judge Schroeder had approved lacked probable cause because the information supporting the warrant was stale. In claiming that the warrant lacked probable cause, the defendant relies primarily on the District Court's

decision in *United States v. Jeff Coon*, 2011 WL 1871165 (W.D.N.Y.), which involved a search warrant affidavit with reference to only one video of child pornography that had been distributed by the defendant in that case. The defendant further claims that the agent who obtained the search warrant did not act in good faith, as he was the same agent in the *Coon* case listed above. The defendant's motion should be denied, as the search and seizure of the defendant's computer were conducted in accordance with the Fourth Amendment, in that the search was conducted pursuant to a warrant duly issued by a neutral Magistrate, that the warrant was supported by probable cause, and further that the warrant was relied upon in good faith. *See Illinois v. Gates*, 462 U.S. 213 (1983); *United States v. Leon*, 468 U.S. 897 (1984).

MAGISTRATE JUDGE'S REPORT AND RECOMMENDATION

Magistrate Judge Scott issued a three-part Report and Recommendation related to the defendant's motion to suppress evidence based upon: (1) the claimed lack of probable cause to support the search warrant, (2) the alleged lack of good faith by the agent in obtaining the search warrant, and (3) the motion to suppress statements of the defendant that were allegedly coerced. With respect to the issue of probable cause for the search warrant, relying primarily on the decision issued in *United States v. Jeff Coon*, 2011 WL 1871165 (W.D.N.Y.), Magistrate Judge Scott found that

probable cause did not exist to support the search warrant in this matter. [Magistrate Judge's Report and Recommendation (MJ R&R) of April 5, 2013, p. 21.]. The Report and Recommendation found that the information contained in the search warrant was "stale and uncorroborated." [MJ R&R, p. 19]. Furthermore, because the Magistrate Judge found that the circumstances in this case were deemed to be similar to the *Coon* case, the Report and Recommendation concluded that the agent was "grossly negligent" in making the search warrant application in that the agent provided two pieces of supposedly "misleading" information to Magistrate Judge Schroeder in the search warrant application and included "boilerplate" language that did not apply. [MJ R&R, p. 25]. Thus, the Report and Recommendation found that good faith was not present, due to the agent's prior involvement in the *Coon* case, where he should have known that the information was stale, and consequently the motion to suppress the search warrant evidence was granted. [MJ R&R, pp. 24, 25]. As for the defendant's statements made to agents at the time of the execution of the search warrant, the Report and Recommendation simply deemed these statements to be "fruit of a poisonous tree" without further analysis. [MJ R&R, p. 25].

The government respectfully submits that the Report and Recommendation that finds the search warrant to be stale based on

the *Coon* decision significantly overlooks various Circuit Court precedent to the contrary, as well as the guidance of the Supreme Court in *Illinois v. Gates*, *supra,* in determining probable cause regarding searching for evidence of a crime. Furthermore, the Report and Recommendation further disregards the holding espoused by the Supreme Court in *Hudson v. Michigan*, 547 U.S. 586 (2006), where it was noted that suppressing evidence "has always been our last resort, not our first impulse." *Hudson v. Michigan*, 547 U.S. 586 (2006).

FACTS

On or about January 13, 2011, in an undercover capacity, ICE SA Eric Sajo of the Special Agent in Charge (SAC) San Diego Cyber Crimes Unit identified a website link posted on the website, www.motherless.com within the "boards" section of the website. The motherless.com "boards" section was an anonymous message board where individuals could post and discuss any topic, mostly regarding sexuality and pornographic material. The message "Say whatever you want, and it doesn't matter, because no one knows who you are!" was posted under "Anonymous Message Boards" header. The suspect web link was found under the "Motherless" category, which annotates "Anything related to this site, found bugs, feature requests, complaints, or other site related materials." The suspect message thread contained the link http://0000chan.cz.cc,

which was anonymously posted on motherless.com boards "motherless" section. SA Sajo clicked on the link and identified an image board entitled "0000chan". The image board was marked "Cool Image Board. Copyright 2010, coolib.org." The top of the webpage allowed a user to enter a name, subject, text and upload four (4) images at a time. The image upload boxes allowed the user to browse, identify the file on the user computer and post the image or images to the main board with the click of the "post" button. Some of the images posted to the Cool Image Board were described as follows:

a. Posted by "edangle" 2011-01-13 11:10:57 #0000014726: The image depicts an underage pre-teen female child. The female child is nude from the waist down wearing a pink and white shirt. The female child is lying on a bed with both legs spread towards the camera. The female child's legs are raised as she spreads her vaginal area with both of her hands. The female child's vaginal area is completely exposed.

b. Posted by "edangle" 2011-01-13 11:14:21 #0000014729 The image depicts two underage pre-teen female children lying on a bed. One female child is lying on her back wearing a pink dress and thigh high white stockings. The pink dress is pulled up to her waist exposing her vaginal area. The second child in the picture is lying on top with her head towards and facing the other female child's vaginal area. The second

female child is wearing a red top with a white headband. The second child appears to be performing oral copulation on the other female child with her tongue on or near the other female child's vagina.

c. Posted by "Anonymous" 2011-01-13 11:26:03 #0000014738 The image depicts an underage pre-teen female child. The female child is naked from her midsection up and is lying on a bed. The female child's left hand is covering her left breast and her right breast is exposed. The female child has what appears to be adult male ejaculate on her face, nose and mouth.

The bottom of the image board page had page numbers, which identified "0-7" pages. The bottom of the page was also marked "Cool Image Board is a work in progress. Keep in mind that it is free. Bugs? Questions? Help?! moderator@coolib.org. Hyperlinks included "home," "Log Out," and Admin Login."

On or about January 14, 2011, SA Sajo conducted a publicly-available domain name query of www.coolib.org, which revealed some of the following information: (1) the domain name coolib.org was created on May 23, 2010; (2) the registrant’s name was listed as Celeste Hensley of Westfield, North Carolina; and (3) the tech

organization for the website was listed as hostgator.com, located at 11251 Northwest Freeway Suite 400, Houston, TX 77092.

On or about February 8, 2011, SA Sajo applied for and obtained a federal search warrant for the website content for coolib.org located in the Southern District of Texas for evidence of violations of Title 18, United States Code, Sections 2252 and 2252A related to child pornography offenses. Evidence obtained pursuant to the search warrant served upon Host Gator at their Houston offices consisted of approximately 861 suspect child pornography files located in image Directory 55 of www.coolib.org and web access log information for images posted to the website.

Host Gator also supplied SA Sajo with a matched entry text document, which separated Internet Protocol (IP) logs with "GET" requests, which were generated when a user's web browser requests/accesses a file from the website to specified images of Directory 55. The evidence obtained from www.coolib.org was obtained for January 16, 2011, due to web server configuration. The web access logs from this website indicated when a user accessed the website and the specific files the user accessed and received, or attempted to receive. A review of the web access logs for the IP address assigned to the user at the relevant time revealed that the user accessed the website and obtained numerous

visual depictions of minors engaged in sexually explicit conduct. Although there is no record that the user accessed an enlarged (full size) image, the logs show more than one incidence of access of thumbnail images by the user. The thumbnail images, as displayed, were of sufficient size for a user to identify the nature and content of the images.

A sample of the web access logs is demonstrated below:

```
67.252.174.8
--------------------
67.252.174.8 - - [16/Jan/2011:07:03:17 -0600] "GET
/coolib/boards/0000000055/im/oKoRiPO8Enid.jpg HTTP/1.1" 200 151199
"http://www.coolib.org/coolib/board.php?id=0000000055" "Mozilla/5.0
(Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13) Gecko/20101203
Firefox/3.6.13"
```

On July 5, 2011, San Diego SA Sajo formally requested information from Time Warner Cable for subscriber information for IP address 67.252.174.8 on January 16, 2011, at 07:03:30-0600 CST. This IP address was associated with the website http://www.coolib.org on the date and time listed as determined through the web access logs for the website. On July 13, 2011, Time Warner Cable provided information that identified James Raymonda as the subscriber for the Internet service related to IP address 67.252.174.8 on January 16, 2011. The residential address associated with IP address 67.252.174.8 was listed by Time Warner Cable as 73 Henley Road, Buffalo, New York 14216. The United States Postal Service confirmed that James Raymonda was receiving mail at this address. Record checks indicate that James Raymonda

and Rachel Lyons were the co-owners of the residence. During surveillance of the residence on October 20, 2011, a wireless check was performed where no open networks were discovered in front or beside the residence from the street.

Internet Protocol (IP) log information for January 16, 2011, identified that the user of IP address 67.252.174.8, James Raymonda, successfully viewed suspect child pornography images contained in Directory 55. The log files also identified the frequency of successful (GET) requests for the suspect images, which provide evidence that the user intended to view the content. The viewable thumbnails as displayed on the message board webpage page are large enough to identify the image content without clicking on the image to enlarge. Each web page captured displayed approximately (30) or less images.

The following web access logs and corresponding tables provide information regarding two of the 76 images, the majority of which were images of child pornography, that were accessed by the user of IP address 67.252.174.8 on January 16, 2011:

(1) 67.252.174.8 - - [16/Jan/2011:07:03:17 -0600] "GET /coolib/boards/0000000055/im/8oteqetU5Aju.jpg HTTP/1.1" 200 317601 "http://www.coolib.org/coolib/board.php?id=0000000055" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13"

Filename	Access Date	Description
"8oteqetU5Aju.jpg"	01/16/2011	An image depicting a nude minor female bent over in such a way as to display her genitals to the camera.

(2) 67.252.174.8 - - [16/Jan/2011:07:03:16 -0600] "GET /coolib/boards/0000000055/im/aVApeXAriBU4.jpg HTTP/1.1" 200 161308 "http://www.coolib.org/coolib/board.php?id=0000000055" "Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13"

Filename	Access Date	Description
"aVApeXAriBU4.jpg"	01/16/2011	An image depicting a minor female who appears to be being penetrated by a nude male adult.

On October 27, 2011, Magistrate Judge Schroeder approved the search warrant for computer equipment and other electronic media related to evidence of a crime involving the possession and receipt of child pornography located at the James Raymonda residence in Buffalo where he accessed in order to download the multiple images of child pornography from the Cool Image Board. On November 8, 2011, HSI SAC Buffalo agents executed a federal search warrant issued in the Western District of New York for 73 Henley Road, Buffalo, New York 14216. At the time of the execution of the search warrant, James Raymonda was encountered inside the residence where he lived with Ms. Lyons and two young children and agreed to

speak with HSI agents, as he was not in custody nor under arrest at the time. In the course of entering one of the agents' vehicles to engage in an interview, Raymonda hit his head on the car door. After being given medical gauze to stop the bleeding, Raymonda agreed to be interviewed by agents.

Raymonda stated to the agents that he used websites like "motherless" and "4chan" to view child pornography. Raymonda was shown screen shot images from the website http://www.coolib.org, and Raymonda stated to agents that it looked familiar to him. Raymonda was shown a printout of some of the images that were determined to have been previously accessed by the user of IP address 67.252.174.8. Raymonda confirmed to agents that he had seen and remembered one of the images which he then initialed and dated. The image is identified as file "iVAMeToTO2a2.jpg" and depicts a minor female who is naked with her legs spread exposing her genitals to the camera. The image has the "LS-Magazine" watermark on the top left of the image, which identifies an Eastern European group known to have created child pornography.

The items of electronic media seized pursuant to the warrant were forensically examined by an HSI computer forensic agent. The results of the forensic examination of the Acer laptop belonging to Raymonda revealed that it contained hundreds of images of child

pornography, that is images of minor children, some of whom are prepubescent children, engaged in sexually explicit conduct, as defined in Title 18, United States Code, Section 2256(8). Another Toshiba laptop, a Generic Tower computer, and Simpletech external hard drive belonging to Raymonda were forensically examined and found to contain over one thousand images of child pornography, as well as evidence that Raymonda had accessed the motherless.com website.

THE SUPPRESSION HEARING

At the evidentiary hearing in this matter which took place on August 7, 2012, October 18, 2012, and November 14, 2012, the government presented the following witnesses from Homeland Security Investigations (HSI): Cybercrimes Special Agent Adam Ouzer, Cybercrimes Special Agent Christopher Bennett, Assistant Special Agent in Charge Vincent Salvatore (questioned on direct examination by the defense), and Assistant Special Agent in Charge Nicholas DiNicola. The government also presented the testimony of Buffalo Police Officer Jeffrey Jajkowski and Assistant United States Attorney Edward White. The defendant presented the testimony of Gerald Grant, the in-house computer examiner for the Federal Public Defender's Office. The government respectfully submits that the testimony and evidence presented at this hearing clearly established that the search warrant obtained in this matter was

supported by probable cause and that Special Agent Ouzer, the affiant for the search warrant, acted in good faith in obtaining this search warrant. As such, the defendant's motion to suppress the evidence obtained pursuant to the search warrant should be denied. The government further submits that the evidence at the hearing clearly established that the defendant's non-custodial statements to agents during a consensual interview undertaken at the time of the execution of the search warrant were made voluntarily, were taken independently, and should not be suppressed. [Transcript of Suppression Hearing (Tr.) at pp. 27, 116]; *See Green v. Scully*, 850 F.2d 894, 901-902 (2d Cir. 1988).

Specifically during the hearing, Agent Ouzer testified regarding his understanding of the IP logs received in evidence as Government's Exhibit #4. [Tr. at pp. 19-21]. Based upon information provided by the investigating agent in San Diego, CA, where the case originated, the logs set forth in Government Exhibit #4 were believed by Agent Ouzer to demonstrate that the computer located using the IP address belonging to the defendant requested images of child pornography from the server of the coolib.org website. [Tr. at pp. 19-21, 52]. The defense witness, Mr. Grant, testified that the logs indicated that images were sought to be obtained from the server. [Tr. at p. 236]. According to Mr. Grant, there were numerous logs with various commands completed in

different stages. [Tr. at p. 229]. Thus, this testimony reflects that more than one command was made to the server by the defendant. He also testified that if all images were downloaded together, it would come up in the same log. [Tr. at p. 223]. Mr. Grant also testified that he did not know the capacity of the defendant's hard drive and did not examine the defendant's computer, but asserted his belief that files would stay in a temporary cache on a computer for 2 days to one month; he acknowledged that while the images may have taken 17 seconds to download, they were available for later viewing; and he acknowledged that it was possible that the person who accessed the images viewed child pornography, which is itself a crime under 18 U.S.C. §2252A(a)(5)(B). [Tr. at pp. 231, 233].

THE RECOMMENDATION TO SUPPRESS EVIDENCE SHOULD BE REJECTED

The government respectfully requests that the District Court reject the findings set forth in the Report and Recommendation that the search warrant lacked probable cause, that the agent did not act in good faith in obtaining the warrant, and that the statements should be suppressed. The Report and Recommendation places great reliance on the decision in the *Coon* case, where the District Court found that probable cause was lacking from the search warrant affidavit related to distribution of one video file of child pornography from one year before the search warrant was obtained. The Report and Recommendation also draws conclusions from the

testimony of the Public Defender's computer examiner about files on the defendant's computer that the witness had never examined. The government submits that based upon a common sense understanding of computers and the practices of individuals such as the defendant who exhibit a sexual interest in children by viewing and seeking to obtain multiple images of child pornography to be stored on a computer, the findings within the Report and Recommendation should be rejected.

The Search Warrant was Supported by Probable Cause

The government maintains that the search warrant was justifiably issued by Magistrate Judge Schroeder in this matter because it was indeed supported by probable cause. Probable cause exists when based upon all of the circumstances set forth in the affidavit accompanying the search warrant, a judicial officer can reasonably conclude that "there is a fair probability that contraband or evidence of a crime will be found in a particular place." *Illinois v. Gates*, 462 U.S. at 238. As set forth in the search warrant application [Government's Exhibit 5], Agent Ouzer testified that according to the "Get Codes" [Government's Exhibit 4], the user of IP address 67.252.174.8, the subscriber to which was the defendant, requested the image for 76 images (most of which were child pornography) from the coolib.org website server on January 16, 2011. [Tr. at p. 52]. The defendant's witness, Mr.

Grant, an employee of the Federal Public Defender's Office, acknowledged that the "get command" indicates that the web browser related to IP address 67.252.174.8 requested that the website server show or retrieve an image. [Tr. at p. 224]. Mr. Grant further acknowledged that although while it may have taken 17 seconds to download the 76 images of primarily child pornography, the images could be viewed at a later time. [Tr. at p. 231]. Furthermore, that 17 seconds of time reflected the completion of the tasks requested by the user, not the actual time the user necessarily spent on the website perusing child pornography images. [Tr. at p. 229]. The witness further acknowledged the possibility that the individual who accessed the images of child pornography on the website could have in fact viewed the images at that time. [Tr. at p. 233]. It was also confirmed by the witness that the logs indicate that the get commands were successfully completed. [Tr. at p. 229].

The probable cause standard being applied with regard to a search warrant does not require proof beyond a reasonable doubt or even by a preponderance of the evidence. The judicial officer instead is required to apply common sense to make a practical determination regarding whether there is a "fair probability" that evidence of a crime will be found in the specified location. *United States v. Smith*, 9 F.3d 1007, 1012 (2d Cir. 1993) (quoting

Illinois v. Gates, 462 U.S. at 238); *United States v. Irving*, 452 F.3d 110, 125 (2d Cir. 2006).

In *Irving*, the Second Circuit Court of Appeals denied the defendant's claim that information supporting the search warrant of his residence from nearly two years prior to the issuance of the warrant was stale, based upon the nature of the crime involving child pornography. *Id.* The Second Circuit further noted that "in a doubtful case, we accord preference to the warrant." *Id.*, (citing to *Rivera v. United States*, 928 F.2d 592, 602 (2d Cir. 1991)).

In the instant case, the initial information regarding the downloading of child pornography by the defendant using IP address 67.252.174.8 occurred approximately 9 and ½ months before Magistrate Judge issued the search warrant on October 27, 2011, significantly less than the nearly two year period in the *Irving* case. Given the character of the crime involving child pornography, there would be a fair probability that evidence of a crime would be found in the place to be searched after 9 months. *See United States v. Frechette*, 583 F.3d 374, 378 (6th Cir. 2009).

The Seventh Circuit Court of Appeals also recognized that "[i]nformation a year old is not necessarily stale as a matter of law, especially where child pornography is concerned." *United*

States v. Newsom, 402 F.3d 780, 783 (7th Cir. 2005), citing to *United States v. Lacy*, 119 F.3d 742, 745 (9th Cir. 1997). Furthermore, Courts have recognized that a specially trained law enforcement officer should be accorded deference as to his or her probable cause determination, particularly as it may relate to the nature of the offense, such as their experience involving those offenders who collect and retain child pornography. *See United States v. Arvizu*, 534 U.S. 266, 273 (2002); *United States v. Lamb*, 945 F.Supp. 441, 460 (N.D.N.Y. 1996).

The Report and Recommendation's conclusion that the search warrant does not indicate additional criminal conduct overlooks the continuing nature of the crime of possession of child pornography, as well as the secretive behavior of those who download and possess images of child pornography on their computers. (MJ R&R p. 16). Courts have recognized that because the criminal conduct of possession of child pornography "is generally carried out in the secrecy of the home and over a long period, the same time limitations that have been applied to more fleeting crimes do not control the staleness inquiry for child pornography." *United States v. Paull*, 551 F.3d 516, 522 (6th Cir. 2009). In *United States v. Wagers*, 452 F.3d 534 (6th Cir. 2006), the United States Court of Appeals for the Sixth Circuit, following similar decisions of the Second Circuit and Fifth Circuit Courts of Appeals,

recognized "that evidence that a person has visited or subscribed to websites containing child pornography supports the conclusion that he has likely downloaded, kept, and otherwise possessed the material." *United States v. Wagers*, 452 F.3d 534, 540 (6th Cir. 2006) [citing *United States v. Martin*, 426 F.3d 68, 77 (2nd Cir. 2005) and *United States v. Froman*, 355 F.3d 882, 890-891 (5th Cir. 2004)].

Special Agent Ouzer set forth in great detail his understanding and experience regarding the nature of child pornography offenses, as well as his experience and understanding of the attributes common to such offenders. He described that the nature of this offense as frequently involving the desire to acquire multiple images of child pornography in the privacy of one's home behind the anonymity of a computer, and to have the ability retain the images and access them at any time in the future as being highly valuable. The affidavit further noted the characteristics of child pornography offenders, the nature of crimes involving possession and receipt of multiple child pornography images, the use of computers and the Internet to facilitate offenses involving child pornography, and the behavioral patterns of individuals with a sexual interest in children that have been recognized internationally by law enforcement officials and others (see, for example, the findings of participants in the

G8 Global Symposium for Examining the Relationship between Online and Offline Offenses and Preventing the Sexual Exploitation of Children (April 5-7, 2009, University of North Carolina)).

Additionally, the affidavit in support of the search warrant for the computer and electronic media at the defendant's residence set forth in significant detail that the defendant, on January 16, 2011, using IP address 67.252.174.8, navigated a complex Internet site containing an image board that provided access to hundreds of images of child pornography, pinpointed the approximately 76 images, most of which were minors engaged in sexually explicit conduct, that he desired and actively sought to view and save them to his computer, which he in fact did. As such, it was not unreasonable for Agent Ouzer or Magistrate Judge Schroeder to believe that there would be a fair probability that evidence of possessing or receiving child pornography would still be present at this residence 9 and ½ months later. *United States v. Martin*, 426 F.3d at 86-87; *United States v. Lacy*, 119 F.3d at 746.

The affidavit described the investigative efforts in great detail, that upon discovering the information regarding the website access logs in January 2011 that involved the defendant's IP address, the Homeland Security agents spent the next several months analyzing the volumes of information obtained. After the

subscriber information was learned in July 2011, it was determined that the user of IP address 67.252.174.8 was located in the Western District of New York. While other criminal activity was not presented in the affidavit, the conduct depicting the series of transactions involving the accessing of 76 images from a child pornography image board consisting primarily of minor children engaged in sexually explicit acts, coupled with the nature of the offenses described involving an individual seeking to collect so many images of children engaged in sexual acts, provided a sufficient basis for the issuance of the warrant by Magistrate Judge Schroeder, just 9 and ½ months after those transactions. The affidavit further outlined that use of computers to facilitate this offense, allowing the images of child pornography to be retained for long periods of time and for such users to seek to avoid detection of their crime. Furthermore, the affidavit noted the ability of forensic experts to locate child pornography material on a computer as being in the user's possession. *See United States v. Patt,* 2008 WL 2915433 (W.D.N.Y. 2008).

The government further notes that in *United States v. Jeff Coon*, the District Court found it to be "a very close case" that involved the downloading by German Police of one video file from the defendant's IP address nearly one year prior to the search warrant. *United States v. Jeff Coon*, 2011 WL 1871165, p. 4

(W.D.N.Y.). The instant case involves the accessing of close to 76 images of child pornography from a website bulletin board devoted to child pornography, and that the related search warrant affidavit contained information that such collectors of child pornography tend to maintain their collections for years. [Government's Exhibit 5]. Despite the Report and Recommendation's finding to the contrary, the affidavit for the search warrant in this case contained far more information to support the contention that there was probable cause to believe that evidence of a crime would be found in the residence of the user of IP address 67.252.174.8 who had accessed coolib.org to access and retrieve images of child pornography. While the Report and Recommendation points to allegedly misleading statements made to the Magistrate Judge (MJ R&R p. 16), the government notes that the affidavit did not assert that the subject distributed child pornography, only that the subject exhibited the characteristics generally of someone who is involved in the distribution, receipt and possession of child pornography. The Report and Recommendation also notes that "there was no evidence to suggest that Raymonda was a pedofile [sic]" (MJ R&R p. 16); however, the affidavit does reflect that an individual who views and receives multiple images of child pornography, which even the defense witness conceded occurred here, is someone with a sexual interest in children. [See Government's Exhibit #5, p. 21]. Thus, the statements from the search warrant affidavit noted in the

Report and Recommendation as "misleading" were in fact supported by the circumstances of the defendant's activity with respect to the accessing of the child pornography images and the multiple requests to the server to obtain images of child pornography.

In reviewing the decisions of various Circuit Courts, the government notes that these decisions generally reflect a common sense understanding of the capabilities of computers and digital evidence when it comes to cases involving child pornography. For instance, the Seventh Circuit Court of Appeals recently noted in a case that appears to undercut the rationale in *Coon*:

> "[s]taleness is highly relevant to the legality of a search for a perishable or consumable object, like cocaine, but rarely relevant when it is a computer file.... Because of overwriting, it is *possible* that the deleted file will no longer be recoverable from the computer's hard drive. And it is also *possible* that the computer will have been sold or physically destroyed. And the longer the interval between the uploading of the material sought as evidence and the search of the computer, the greater these possibilities. But rarely will they be so probable as to destroy probable cause to believe that a search of a computer will turn up the evidence sought; for probable cause is far short of certainty-"

United States v. Seiver, 692 F.3d 774, 777 (7th Cir. 2012). The Court further noted that "seven months is too short a period to reduce the probability that a computer search will be fruitful to a level at which probable cause has evaporated." *Id.* In the

instant case, the government would submit that 9 and ½ months is likewise too short a period for probable cause to disappear.

In *United States v. Kain*, the Eighth Circuit noted that "the presence of child pornography in temporary internet and orphan files is *evidence* of prior possession of that pornography..." and that "[a] computer user who intentionally accesses child pornography images on a web site gains control over the images, just as a person who intentionally browses child pornography in a print magazine "knowingly possesses" those images, even if he later puts the magazine down..." *United States v. Kain*, 589 F.3d 945, 950 (8th Cir. 2009) (emphasis in the original). The Court noted that Congress intended to criminalize the viewing of child pornography images in enacting 18 U.S.C. § 2252A(a)(5)(B). *Id.*

The Second Circuit noted in *United States v. Ramos*, that with respect to images stored in temporary internet files, the defendant in that case "had some control over the images even without saving them - he could view them on his screen, he could leave them on his screen for as long as he kept his computer on, he could copy and attach them to an email and send them to someone, he could print them, and he could (with the right software) move the images from a cached file to other files and then view or manipulate them offline." *United States v. Ramos*, 685 F.3d 120, 131-132 (2d Cir.

2012). The Court further noted that "an individual who views images on the internet accepts them onto his computer, and he can still exercise dominion and control over them, even though they are in cache files. In other words, he receives and possesses them." *Id*. at 132. With the images in his internet cache, defendant Raymonda could have taken the actions noted above when he accessed the images from the internet in January 2011, providing further evidence of receipt and possession of child pornography as sought in the search warrant.

Accordingly, the government respectfully submits that the application for the search warrant in this action was sufficiently supported by probable cause, and that the Report and Recommendation that recommends granting the defendant's motion to suppress the computer evidence seized pursuant to that warrant should be rejected on that basis.

The Search Warrant was Relied Upon in Good Faith

The government further submits that the Report and Recommendation was erroneous in not finding that the search of the defendant's computer fell within the good faith exception to the exclusionary rule. *United States v. Leon*, *supra*. The Report and Recommendation finds that the search warrant application was lacking in indicia of probable cause to render the agent's reliance

upon it as unreasonable because of his involvement in the *Coon* case, and that the warrant contained 2 alleged pieces of misleading information. As set forth above, the affidavit in support of the search warrant in the instant case was not a bare bones affidavit, but to the contrary, provided significant indicia of probable cause to support the search of the defendant's computer. Agent Ouzer acted in an objectively reasonable manner in reliance upon the warrant, given the significant information developed throughout the course of the lengthy investigation, despite the defendant's attempts to tie this agent to the other cases that were subject to failed motions to suppress the child pornography evidence (*United States v. Coon, supra*). Furthermore, the finding that the 2 pieces of supposedly misleading information were present in the warrant affidavit is undermined by the testimony of Mr. Grant, in that he confirmed that numerous commands were made to the server by the defendant to show or retrieve images of child pornography and that the agent did not allege that the defendant actually distributed child pornography. As such, the basis to find that the Magistrate Judge was misled is undercut by the testimony of the defendant's witness.

With regard to the *Coon* case, Agent Ouzer testified that he was unaware of the various rulings of the Court in the *Coon* case that probable cause was lacking (or not) with respect to the search

warrant for the Coon residence. [Tr. at pp. 76-77]. Supervisory Agents Salvatore and DiNicola both testified that they were not informed or aware of the Court's ruling in the *Coon* case as well. [Tr. at pp. 189, 267]. Furthermore, Assistant U.S. Attorney White testified that he did not discuss the details of the staleness argument raised by the defense in the *Coon* case with Agent Ouzer. [Tr. at pp. 282, 300]. As demonstrated by the testimony of Agents Ouzer, Salvatore, and DiNicola and Assistant U.S. Attorney White, it is clear that the specifics of the staleness claims raised in the *Coon* case were not known by Agent Ouzer at the time he applied for the search warrant in this case, and that Mr. Coon had pled guilty to possession of child pornography on September 11, 2011, several weeks before Agent Ouzer even received the lead from the San Diego agent regarding the Raymonda case. While the government maintains that the proceedings in the *Coon* case were nevertheless irrelevant to this case, as there was greater indicia of probable cause present in this case, the finding in the Report and Recommendation of a lack of good faith as to Agent Ouzer because of his involvement in the *Coon* case is erroneous, particularly in light of the fact that the *Coon* case was a very narrowly held decision and the fact that even this Court flip-flopped in its decision about whether probable cause existed to support the Coon search warrant. As such, in light of Agent Ouzer's understanding of the probable cause requirement, and his lack of knowledge of the

details of the nuances of the probable cause issues germane only to the narrowly-decided *Coon* case, it was error to determine that the agent was grossly negligent in seeking this search warrant. The government does agree that the agent's conduct was neither reckless nor intentional under the standard set forth in *Herring v. United States*, 555 U.S. 135 (2009).

The affidavit in this case sets forth in substantial detail many objective facts, including the access and navigation of a series of complex child pornography websites, the series of transactions engaged in by the user of IP address 67.252.174.8 to view approximately 76 images of children, including prepubescent children, engaged in sexually explicit conduct, the nature of the continuing offense of child pornography receipt and possession where images are actively downloaded to the user's computer and perhaps saved for long periods, and the agent's experience related to the investigation of such crimes, all of which would support a finding that the agent acted in good faith in relying upon the warrant to execute the search of the defendant's computer. *United States v. Clark,* 638 F.3d 89, 100 (2d Cir. 2011); *United States v. Moore,* 968 F.2d 216, 222 (2d Cir. 1992); *United States v. Pappas,* 592 F.3d 799, 802 (7th Cir. 2010).

Accordingly, the Report and Recommendation finding that the agent lacked good faith in obtaining the search warrant for the defendant's computer media in this case should be rejected.

The Defendant's Statements were Independent of the Search

The evidence and testimony presented at the hearing sufficiently demonstrated that the defendant was not in custody at the time he was interviewed by agents, nor was he coerced into making any statements. Agents Ouzer and Bennett both testified that Raymonda was free to leave but chose to stay and talk with agents. [Tr. at pp. 27, 116]. While the Report and Recommendation refers to the statements made in the car to agents as "fruit" of the unlawful search (MJ R&R p. 25), the government notes that the defendant freely chose to stay with agents instead of leaving the premises, went to the car and talked with agents despite hitting his head on the car door, and made spontaneous statements to agents which were not as a result of being questioned, which were attenuated from the search and were not the result of the search. *See Wong Sun v. United States*, 371 U.S. 471, 492 (1963). The government requests that should the search be found to be supported by probable cause or the warrant relied upon in good faith, the voluntary statements of the defendant should not be suppressed, as no coercive government conduct was present so as to render the statements involuntary. *Colorado v. Connelly*, 479 U.S. 157, 165

(1986). In any circumstances, the defendant's excited utterances that he wanted agents to put a bullet in his head and that he had nothing to live for, which were spontaneously made upon learning that his wife and children were leaving, should not be suppressed, as these statements were not the result of the search or even any questioning of the defendant. *Hudson v. Michigan*, 547 U.S. at 592, 593.

CONCLUSION

Based upon the foregoing, it is respectfully submitted that the Magistrate Judge's Report and Recommendation granting the defendant's motion to suppress evidence and the defendant's statements as "fruit of the poisonous tree" should be rejected in all respects.

DATED: Buffalo, New York, April 19, 2013.

Respectfully submitted,

WILLIAM J. HOCHUL, JR.
United States Attorney

S/ FAUZIA K. MATTINGLY

BY: _____

FAUZIA K. MATTINGLY
Assistant United States Attorney
United States Attorney's Office
Western District of New York
138 Delaware Avenue
Buffalo, New York 14202
716/843-5831
Fauzia.Mattingly@usdoj.gov

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA	
v.	11-CR-397-S
JAMES RAYMONDA,	
Defendant.	

CERTIFICATE OF SERVICE

I hereby certify that on April 19, 2013, I electronically filed the foregoing **GOVERNMENT'S OBJECTIONS TO THE MAGISTRATE JUDGE'S REPORT AND RECOMMENDATION** with the Clerk of the District Court using its CM/ECF system, which would then electronically notify the following CM/ECF participant(s) on this case:

Kimberly A. Schechter, Assistant Federal Public Defender

S/ FAUZIA K. MATTINGLY

FAUZIA K. MATTINGLY